Schäfer, Günter:

Fachgebiet Telematik/Rechnernetze an der Technischen Universität Ilmenau

URN: urn:nbn:de:gbv:ilm1-2015210304

Published OpenAccess: January 2015

Original published in:

Praxis der Informationsverarbeitung und Kommunikation : PIK. - Berlin : de Gruyter (ISSN 1865-8342). - 31 (2008) 3, S. 202-204.
DOI: 10.1515/piko.2008.0034
URL: http://dx.doi.org/10.1515/piko.2008.0034
[Visited: 2015-01-20]

FACHGEBIET TELEMATIK/ RECHNERNETZE AN DER TECHNISCHEN UNIVERSITÄT ILMENAU

Prof. Dr.-Ing. Günter Schäfer

Das Fachgebiet Telematik/Rechnernetze der Fakultät für Informatik und Automatisierung an der Technischen Universität Ilmenau wird seit April 2005 von Günter Schäfer geleitet und besteht zur Zeit neben seinem Leiter aus drei wissenschaftlichen Mitarbeitern und einem externen Doktoranden.

Im Bereich der Lehre bietet das Fachgebiet ein breites Spektrum an Vorlesungen zur Telematik und Rechnernetzen an, das grob in die drei Bereiche Grundlagen (Telematik 1, Telematik 2, Leistungsbewertung, Grundlagen der Telematik), Netzsicherheit (Network Security, Schutz von Kommunikationsinfrastrukturen) und weitere Spezialvorlesungen (Advanced Networking Technologies, Multimedia Information Retrieval, Öffentliche Netze) eingeteilt werden kann. Neben vertiefenden Praktika, Projekt- und Hauptseminaren zu diesen Themen rundet eine Anfängervorlesung im Bachelorstudiengang Informatik über Algorithmen und Programmierung das Lehrangebot des Fachgebiets ab.

Die aktuellen Forschungsschwerpunkte des Fachgebiets können kurz durch die folgenden Stichwörter charakterisiert werden:

- Schutz von Kommunikationsinfrastrukturen,
- Innovative Protokolle, Architekturen und Anwendungen mobiler und ubiquitärer Systeme sowie
- Peer-to-Peer basierte Unterstützung von Multimedia-Streaming-Anwendungen

In allen Gebieten ist es das Ziel, neue Protokollmechanismen und Implementierungskonzepte zu entwickeln, prototypisch zu realisieren, sowie Kenngrößen aus dem praktischen Einsatz zu ermitteln.

Schutz von Kommunikationsinfrastrukturen

Es ist eine mittlerweile wohlbekannte Tatsache, dass die digitale Revolution und die allgegenwärtige Vernetzung von Informationssystemen bei all ihren Vorteilen auch einige Risiken mit sich bringt. Mit der zunehmenden Integration von Informations- und Kommunikationssystemen in nahezu alle Bereiche des privaten, gesellschaftlichen und geschäftlichen Lebens steigt in modernen Informationsgesellschaften insbesondere die Abhängigkeit von der Verfügbarkeit und korrekten Funktion der diesen Diensten zugrunde liegenden Kommunikationsinfrastrukturen. Als immer größere Bedrohung erweisen sich in diesem Zusammenhang vorsätzliche Sabotageangriffe auf grundlegende Kommunikations- oder Systemdienste.

Aus dem hohen Risikopotential von Angriffen für jetzige wie zukünftige Netzinfrastrukturen ergibt sich somit insgesamt eine ständig steigende Bedrohung, der angemessen entgegnet werden muss. Das gilt in verstärktem Maße bei Vereinheitlichung der verwendeten Kommunikationsprotokolle, wie sie etwa derzeit durch die zunehmende Einführung IP-basierter Komponenten in die Netzinfrastruktur angestrebt wird (siehe z.B. Voice over IP, zukünftige Releases der UMTS-Standards).

Es besteht somit ein dringender Bedarf dafür, systematische Bedrohungsanalysen durchzuführen und einen abgestimmten Maßnahmenkatalog zu entwickeln, der es erlaubt, herkömmlichen Angriffen auf die Vertraulichkeit und Integrität übertragener Daten ebenso wie vorsätzlichen Sabotageangriffen effektiv zu begegnen und der sowohl kryptographische Maßnahmen (Verschlüsselung, Integritätssicherung, Authentisierung, „Client Puzzles“ etc.) als auch netzwerktechnische Maßnahmen (Traceback, Paketfilterung, Intrusion Detection, aktive Netztechnologien etc.) umfassen wird. Hierbei ist jedoch zu gewährleisten, dass die Leistungseigenschaften der Kommunikationsdienste nicht über Gebühr beeinträchtigt werden. Insbesondere ist zu untersuchen, wie angemessene Schutzmechanismen so in Systeme der Kommunikationsinfrastruktur integriert werden können, dass die Dienstgüteanforderungen (Quality of Service, QoS) weiterhin eingehalten werden können.

Am Fachgebiet Telematik/Rechnernetze werden zur Zeit in Kooperation mit einem Industriepartner automatische Mechanismen zur sicheren Konfiguration von IPsec-Infrastrukturen entwickelt, da die IPSec-Gateways zurzeit oftmals noch manuell oder über zentrale Server konfiguriert werden. Dies führt in großen Netzwerken zu Skalierbarkeitsproblemen und ist darüber hinaus fehlerträchtig.

Der entwickelte Ansatz SOLID (Secure OverLay for IPSec Discovery) versucht die Ziele klassischer Routing-Protokolle, wie Skalierbarkeit und Robustheit, zu erfüllen ohne die Sicherheitsziele von IPSec zu verletzen. Dazu formen die IPSec-Gateways ein strukturiertes Overlay-Netzwerk, mit dem sie in der Lage sind, andere Gateways auch dann zu finden, wenn noch kein Security Policy Database Eintrag existiert und die IPSec-Gateways ein verschachteltes Netzwerk mit privaten Adressbereichen bilden.

In umfangreichen Simulationsstudien wurde bereits die Skalierbarkeit und Robustheit des Verfahrens nachgewiesen, so dass inzwischen ein Prototyp für Linux-basierte Systeme entwickelt wird. Ferner befinden sich verschiedene Erweiterungen zur Unterstützung von mobilen IPSec-Gateways und Mandatory Access Control in der Konzeptionsphase.

Innovative Protokolle, Architekturen und Anwendungen mobiler und ubiquitärer Systeme

Auf dem Gebiet der Telekommunikationsnetze haben sich in den letzten Jahren eine Vielzahl von Entwicklungen vollzogen, die insgesamt zur kostengünstigen Bereitstellung einer für die meisten Anwendungen ausreichend hohen Bandbreite im Festnetzbereich und zur allgegenwärtigen Verfügbarkeit von Mobilkommunikationsdiensten geführt haben. Bei den Mobilkommunikationsnetzen herrscht derzeit noch die Situation vor, dass entweder eine ausreichend hohe Bandbreite bei eingeschränkter Mobilitäts- und QoS-Unterstützung (WLAN) oder ausreichende Mobilitäts- und Dienstgüteunterstützung bei eingeschränkter Bandbreite (GSM, UMTS) zur Verfügung stehen; bereits begonnene Bestrebungen zur Integration dieser Netzkonzepte sollen zukünftig jedoch immerhin einen nahtlosen Übergang zwischen den zueinander komplementären Technologien ermöglichen, wobei hierbei noch eine Reihe von Fragestellungen bezüglich der Integration von Sicherheitskonzepten und der effizienten und koordinierten Realisierung von Handovern zwischen unterschiedlichen Zugangsnetzen zu lösen sind. Qualitativ wird diese Entwicklung vor allem durch den Beginn der Konvergenz sowohl von Protokollen der klassischen Telekommunikation und der Internet-Protokollfamilie als auch von Festnetz- und Mobilkommunikation begleitet, wobei zu erwarten ist, dass dieser Konvergenzprozess auch in der Zukunft fortgeschrieben wird.

In Kooperation mit einem Unternehmen wurde am Fachgebiet das Mobilitätsma-

10.1515/piko.2008.0034

nagement für ein Mobilfunknetz der künftigen Generation unter besonderer Berücksichtigung der Vielfalt an potentiellen Zugangstechnologien untersucht. Für eine reibungslose Integration der einzelnen heterogenen Zugangstechnologien sind dabei auch einige Modifikationen im Kernnetz des Mobilfunkbetreibers nötig, wie zum Beispiel der durchgängige Einsatz von IP und damit verbunden auch ein IP-basiertes Mobilitätsmanagement. Damit wird sichergestellt, dass Kommunikationsendpunkte auch nach vertikalen Handovern, also Mobilität über Grenzen unterschiedlicher Zugangstechnologien hinweg, bestehen bleiben. So sollte zum Beispiel ein Handover von WLAN zu UMTS den Empfang eines Videodatenstroms auf einem mobilen Endgerät nicht beeinträchtigen.

Das gegenwärtige Standardprotokoll für Mobilitätsmanagement ist Mobile IP, welches jedoch einige Schwächen aufweist, wie zum Beispiel eine eher zentralistische Struktur und die feste Bindung eines mobilen Gerätes an einen einzelnen Server. Um diese Restriktionen zu umgehen, wurde im Rahmen der Kooperation der Distributed IP Mobility Approach (DIMA) entwickelt. DIMA basiert auf Mobile IP und verteilt die Funktionalität der zentralen Komponenten über ein Overlay-Netzwerk basierend auf einem Distributed Hash Table (DHT). Es bietet eine Netzwerk-basierte Routen-Optimierung und eine verbesserte Ausfallsicherheit. Dabei wird ein geringfügig höherer Signalisierungsaufwand in Kauf genommen. Zur Analyse des Verfahrens wurden umfangreiche Simulationsstudien durchgeführt und die Skalierbarkeit des Systems untersucht.

Parallel zu den zuvor beschriebenen Entwicklungen im Bereich der Mobilkommunikationsarchitekturen zeichnet sich in den vergangenen Jahren weiterhin ein Trend von der rein Mensch-bezogenen Kommunikation (z.B. Telefonie, Internet-Nutzung) hin zur Maschinen-getriebenen Kommunikation, um auf dieser Grundlage zahlreiche Überwachungs- und Steuerungsanwendungen zu realisieren.

Ein aktuell sehr intensiv bearbeitetes Forschungsfeld ist in diesem Zusammenhang die Kommunikation von Fahrzeugen untereinander zur frühzeitigen Erkennung von Gefahrensituationen und allgemeinen Verbesserung des Verkehrsflusses. Die in diesem Kontext derzeit in der Entwicklung befindlichen Vehicular Ad-Hoc Networks müssen für einen verlässlichen Betrieb jedoch gegen Einspielung von falschen Informationen gesichert werden. Besonders die ausgetauschten Positionsinformationen müssen zuverlässig sein, da sie für Applikationen und teilweise auch die Nachrichtenweiterleitung benötigt werden.

In den Arbeiten des Fachgebiets wurde im Rahmen einer Kooperation mit einem Industriepartner das Problem der vorsätzlichen Fälschung von Positionsinformationen durch potentielle Angreifer systematisch untersucht. Im ersten Schritt wurden hierbei die Motivation und die einem Angreifer zur Verfügung stehenden Angriffstechniken diskutiert. Um den identifizierten Bedrohungen entgegenzuwirken, wurde ein System entworfen, das eine Analyse und anschließende Bewertung von Verhaltensmustern von Fahrzeugen vornimmt. Hierzu untersucht das System autonom verschiedene Charakteristiken, wie z.B. Geschwindigkeit und Beschleunigung, was unter anderem auch durch bordeigene Sensoren wie z.B. Abstandsradar unterstützt wird. Jeder dieser Überprüfungsprozesse wird „Sensor“ genannt, und die Werte der einzelnen Sensoren werden mit Hilfe eines Bewertungsalgorithmus zu einer Gesamteinschätzung kombiniert. Auf der Grundlage definierter Schwellwerte wird dann entschieden, ob ein Fahrzeug als vertrauenswürdig, als nicht vertrauenswürdig oder als nicht bewertbar einzustufen ist. Wenn Fahrzeuge als vertrauenswürdig eingeschätzt werden, erlaubt das System, diese Information anderen Fahrzeugen mitzuteilen und somit Empfehlungen auszusprechen, die von anderen in ihren Entscheidungsfindungsprozess einbezogen werden können. Somit kombiniert das Verfahren die sensorgestützte Überprüfung von Lokationsangaben mit einem Reputationssystem.

Das konzipierte System wurde im Rahmen einer umfassenden Simulationsstudie im Hinblick auf die Qualität und Quantität der aufgebauten Vertrauensbeziehungen sowie die Erkennungsrate von Angreifern untersucht. Im Ergebnis der Studie zeigt sich, dass das System ausreichend viele Vertrauensbeziehungen etablieren kann, um ein genügend dichtes Vertrauensnetzwerk herzustellen. Insbesondere durch Verwendung von Empfehlungen ist dies sogar in weniger dichten Verkehrsszenarien möglich. Ortsfeste Angreifer werden dabei mit hoher Erkennungsrate detektiert. Bei Verbesserung der Angriffstechnik, z.B. durch aktive Teilnahme am Straßenverkehr während des Angriffs, wird es für das System schwieriger, eine klare Entscheidung zu treffen. Im Ergebnis erhöht sich jedoch nur die Zeit bis zur Erkennung geringfügig.

Ein weiterer, zurzeit stark wachsender Bereich der maschinengetriebenen Kommunikation wird durch den Einsatz der sogenannten RFID-Technik (Radio Frequency Identification) für die Steuerung und Verwaltung von Warenflüssen forciert. Hierbei werden Güter mit einem so genannten Transponder ausgestattet, der auf Anfragen von Lesegeräten antworten kann und damit eine kontaktlose Übermittlung von Informationen zwischen Gütern und informationsverarbeitenden Systemen ermöglicht.

Am Fachgebiet Telematik/Rechnernetze werden in diesem Zusammenhang Fragen zum sicheren Einsatz von RFID-Lösungen im Supply Chain Management untersucht. Ausgangspunkt dieser Arbeiten ist die Fragestellung, wie eine Architektur gestaltet sein muss, mit deren Hilfe mehrere, ggf. in einigen Bereichen konkurrierende Firmen einer Supply Chain auf gemeinsam genutzte RFID-Chips zugreifen und dort sicher Daten hinterlegen und abfragen können. Motiviert wird der Einsatz gemeinsam genutzter RFID-Chips hierbei sowohl durch die offensichtliche Kostenersparnis als auch durch eine Reihe technischer Vorteile: unter anderem treten weniger Kollisionen an der Funkschnittstelle auf und Lieferbeziehungen können flexibler gestaltet und an neue Bedingungen angepasst werden.

Die erarbeitete Lösung setzt umfangreiche Sicherheitsanforderungen um, so dass beispielsweise nur ein vertrauenswürdiger Dritter die RFID-Tags identifizieren kann und die Privatsphäre der Endkunden geschützt ist, auch wenn beispielsweise ein reklamiertes Produkt wieder in den Warenkreislauf zurückkehrt. Ferner stellt das Verfahren sicher, dass die Kompromittierung einzelner Teilsysteme nur temporäre und lokal begrenzte Auswirkungen hat.

Die sicherheitsrelevanten Eigenschaften des in diesem Kontext entworfenen Protokolls wurden formal auf Schwachstellen untersucht, und darüber hinaus in einer Simulationsstudie die Praktikabilität des Verfahrens am Beispiel eines Supply Chain Szenarios mit mehreren Milliarden RFID-Tags nachgewiesen.

Peer-to-Peer basierte Unterstützung von Multimedia-Streaming-Anwendungen

Zusammen mit der beständig wachsenden, den Endanwendern zur Verfügung stehenden Übertragungsbandbreite steigt die Nachfrage nach multimedialen Diensten. Die Bereitstellung dieser Dienste führt beim Einsatz des herkömmlichen Client-Server-Kommunikationsmodells zu vielfach redundanter Übertragung der Daten und einer sehr hohen Netzlast für den Dienstanbieter. Die hieraus resultierenden hohen Kosten stellen für potentielle Anbieter interessanter Inhalte ein ernstzunehmendes Hindernis dar, einen multimedialen Dienst zur Verfügung zu stellen.

Um dieses Hemmnis aufzuheben sind eine Reihe unterschiedlicher Ansätze vorgeschlagen und implementiert worden, die allerdings ebenfalls insbesondere für Anbieter mit eingeschränktem finanziellen Budget keine Option sind. Zu nennen ist hier vor allem Netzwerk-Multicast, eine Lösung auf der Ebene der Netzwerkschicht, bei der redundante Übertragungen im Prinzip vollkommen vermieden werden könnten, die allerdings nicht in der Anzahl zu unterstützender Gruppen skaliert, da in jedem Router für jede Kommunikationsgruppe ein Zustand vorgehalten werden muss. Weitere verbreitete Lösungen sind die Bereitstellung mittels Server-Farmen oder sogenannter Content Delivery Networks, die jedoch auch einen nicht unerheblichen finanziellen Aufwand bedeuten.

Eine vielversprechende Lösung, die ohne zusätzliche Infrastruktur auskommt und sich der bei den Nutzern vorhandenen Ressourcen bedient, ist der Application-Layer-Multicast (ALM), der häufig auch als kooperatives Multimedia-Streaming bezeichnet wird. Hierbei replizieren die den Datenstrom empfangenden Systeme diesen für andere Systeme, so dass das Angebot an potentiellen Datenquellen für einen bestimmten Datenstrom automatisch mit der Nachfrage nach diesem Datenstrom steigt.

Bei der Realisierung eines ALM-basierten Verteildienstes für die Live-Übertragung multimedialer Daten („Live-Streaming“) sind neben den üblicherweise an Übertragungsdienste für Multimedia-Daten gestellten Dienstgüteanforderungen, wie eine möglichst geringe Ende-zu-Ende-Verzögerung (Delay) und Schwankung dieser Verzögerung (Jitter), auch Anforderungen in Bezug auf die Effizienz der Verteiltopologie zu beachten – letztere wird charakterisiert durch das Verhältnis der Pfadlängen in der Topologie im Vergleich zum kürzesten Pfad (Path Stretch) und die Anzahl von Kopien identischer Pakete auf einzelnen Teilstrecken (Link Stress). Von ebenso großer Bedeutung für einen kommerziellen Einsatz dieses Ansatzes ist jedoch die Gewährleistung einer hohen Verfügbarkeit des Verteildienstes bei zufälligen Störungen sowie bei vorsätzlichen Sabotageangriffen.

In einem von der DFG geförderten Drittmittelprojekt werden am Fachgebiet Telematik/Rechnernetze sowie am Fachgebiet Automaten und Formale Sprachen der TU Ilmenau die Konstruktion sabotageresistenter und effizienter Verteiltopologien untersucht und geeignete Signalisierprozeduren für diese Aufgabe entworfen und bewertet.

Dem Projekt zugrunde liegen Vorarbeiten, die im Rahmen einer 2007 abgeschlossenen Dissertation am Fachgebiet Telematik/Rechnernetze entstanden sind und in denen bereits ein ALM-Streaming-System unter hauptsächlicher Berücksichtigung der Kriterien Stabilität und Effizienz entwickelt wurde. In dem entwickelten Ansatz wird ein Video-Stream in mehrere separate Teildatenströme (Stripes) aufgeteilt und diese jeweils über einen eigenen Spannbaum übertragen.

In dem DFG- Projekt werden aufbauend auf diesen Vorarbeiten erweiterte Fragestellungen untersucht. Das betrifft zum einen die Frage, wie Verteiltopologien in Bezug auf Sabotageresistenz und Netzwerkeffizienz mit möglichst geringem algorithmischen Aufwand bewertet werden können. Zum anderen sollen verteilte Algorithmen zur Topologiekonstruktion entworfen und die resultierenden Topologien in konkreten kommunikationstechnischen Einsatzszenarien in Bezug auf ihr Leistungsverhalten untersucht und experimentell evaluiert werden.

Für weitere Informationen sei auf die Internet-Seiten des Lehrstuhls verwiesen: http://www.tu-ilmenau.de/fakia/telematik.html